



UNP



Plan

DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
GTE-PL-02-V9

Gestión Tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
26-01-2026



Tabla de Contenido

1. OBJETIVO 3

2. ALCANCE.....3

3. DEFINICIONES: 3

4. MARCO LEGAL: 7

5. CONDICIONES GENERALES: 10

6. CONTENIDO..... 11

6.1 Estado Actual de la Entidad respecto al Sistema de Seguridad y Privacidad de la Información SGSI11

6.2 Descripción del Modelo de Seguridad y Privacidad Información MSPI 14

6.3 Para Lograr el Cumplimiento del Plan se Definen las Siguietes Etapas: 16

6.3.1 Contexto 16

6.3.2 Alcance..... 16

6.3.3 Política del MSPI 16

6.3.4 Identificación de Activos de Información 16

6.4 Estrategia de Seguridad Digital..... 17

7. META ESTABLECIDA 19

8. INDICADOR DE MEDICIÓN..... 19

9. HOJA DE RUTA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y ESTRATEGIA DIGITAL (CRONOGRAMA) 21

10. DOCUMENTOS RELACIONADOS:..... 27

11. CONTROL DE CAMBIOS 27

12. CRÉDITOS: 28



1. OBJETIVO

Definir el Plan de Seguridad y Privacidad de la Información, alineado con el MSPI, el MIPG y la normativa vigente con el fin de fortalecer y mejorar el Sistema de Gestión de Seguridad de la Información – SGSI en la Entidad garantizando la confidencialidad, integridad y disponibilidad de la información, el fortalecimiento de los servicios de TI y la protección de los datos institucionales.

2. ALCANCE

El Plan de Seguridad y Privacidad de la Información aplica a los procesos misionales, estratégicos y de apoyo de la Entidad, a los activos de información físicos y digitales, a los servicios tecnológicos institucionales y al personal que administra o utiliza información, incluyendo servidores públicos, contratistas y terceros. En el marco de este plan se implementan acciones orientadas a fortalecer el SGSI, definir lineamientos y responsabilidades, consolidar controles de seguridad, promover la cultura de protección de la información y realizar seguimiento y mejora continua de las prácticas de seguridad, en alineación con el MSPI y el MIPG, garantizando la confidencialidad, integridad y disponibilidad de la información institucional y la continuidad de los servicios.

3. DEFINICIONES:¹

- Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- Activo: En relación con la seguridad de la información, se refiere a cualquier información elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).
- Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como Testimonio e información a la persona o institución que los produce y a los ciudadanos, como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley

¹ Fuente. Modelo de Seguridad y Privacidad de la Información" - Anexo 1 de la Resolución 500 de 2021 de MinTIC
https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf



594 de 2000, art 3).

- Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000)
- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), encargado de coordinar la prevención, mitigación, gestión y respuesta ante incidentes de seguridad digital tanto en el sector público como en el privado. Su objetivo es mejorar las capacidades de respuesta ante amenazas cibernéticas y promover la ciberseguridad
- Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
- Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son



considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos:** Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los



requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Infraestructura Crítica Cibernética (ICC):** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía. (Decreto 338 de 2022). Esta se alinea a la definición de NIST Sistema y activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la salud pública nacional o la seguridad, o cualquier combinación de estos asuntos. NIST SP 800-30 Rev.1
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, amonificación o cifrado.
- **Modelo de Seguridad y Privacidad de la Información - MSPI:** Lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital
- **Partes interesadas (Stakeholders):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **Responsabilidad Demostrada:** Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de



demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).
- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).
- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

4. MARCO LEGAL:

Norma	Número	Año	Descripción - Epígrafe
Ley	1915	2018	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Ley	1712	2014	Ley de transparencia y del derecho de acceso a la información pública nacional
Ley	1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley	1474	2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.



Norma	Número	Año	Descripción - Epígrafe
Ley	1341	2009	Por el cual las Entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones
Ley	1273	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Decreto	338	2022	Establece la gobernanza de la seguridad digital, creando el Modelo y las instancias para fortalecer la ciberseguridad nacional, incluyendo el COLCERT y CSIRT-Gobierno. Sin embargo, dependiendo del contexto
Decreto	1263	2022	Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública
Decreto	767	2022	Por el cual se establecen los lineamientos generales de la Norma de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto	2106	2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública
Decreto	612	2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto	1499	2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
Decreto	1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Decreto	1083	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública
Decreto	1074	2015	por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Capítulo 25 reglamenta parcialmente la ley 1581 de 2012 - Capítulo 26. registro nacional de bases de datos
Decreto	1080	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura. Parte VIII patrimonio bibliográfico, hemerográfico, documental y archivístico. Título II patrimonio archivístico. Título III publicación y divulgación de la información pública- transparencia activa. Título IV gestión de la información clasificada y reservada. Título V instrumentos de la gestión de información pública.
Decreto	4065	2011	Por el cual se crea la Unidad Nacional de Protección (UNP), se establecen su objetivo y estructura.



Norma	Número	Año	Descripción - Epígrafe
Resolución	2277	2025	Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
Resolución	746	2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021.
Resolución	500	2021	Por el cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital. (MinTIC)
Resolución	1519	2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".
Resolución	2250	2025	Por medio de la cual se adopta la Política del Modelo Integrado de Planeación y Gestión – Sistema Integrado de Gestión de la UNP y se deroga la resolución 0649 de 2024
Resolución	2221	2025	"Por medio de la cual se establecen los lineamientos y estándares para la actualización el Anexo 1 de la resolución 500 de 2021 de conformidad con lo dispuesto en la resolución 02277 de 2025 y se derogan otras disposiciones relacionadas con la materia de actualización e incorporación de la estrategia de seguridad digital, en la Unidad Nacional de Protección
Resolución	0928	2025	Por la cual se actualiza el Modelo Integrado de Planeación y Gestión (MIPG-SIG) de la Unidad Nacional de Protección y se dictan otras disposiciones> y se deroga la Resolución 1767 de 2024 "por medio de la cual organiza el Modelo Integrado de Planeación y Gestión (MIPG-SIG) de la Unidad Nacional de protección y se dictan otras disposiciones".
Resolución	1773	2024	Por medio de la cual se establece la Política Integral de Administración de Riesgos de la Unidad Nacional de Protección.
Resolución	0054	2024	Por medio de la cual se actualiza la Plataforma Estratégica de la Unidad Nacional de Protección – UNP para el período 2023 – 2026 y se deroga la Resolución 0199 del 2 de marzo de 2020
Resolución	0932	2023	Por medio de la cual se crea el Grupo de las Tecnologías (GGT) y modifica parcialmente la Resolución número 501 de 2021.
Resolución	2258	2009	Por la cual se modifican los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1.8 y 2.4 de la Resolución CRT 1740 de 2007
Resolución	2460	2022	Por medio de la cual se regula la Norma de Teletrabajo en la Unidad Nacional de Protección, se derogan las Resoluciones 1228 y 1826 de 2021, y se dictan otras disposiciones".
Directiva Presidencial	8	2022	Directrices de austeridad hacia un gasto público eficiente
Directiva Presidencial	4	2012	Eficiencia Administrativa y Lineamientos de la Norma Cero Papel en la Administración Pública.



Norma	Número	Año	Descripción - Epígrafe
CONPES	3995	2020	Política Nacional de Confianza y Seguridad digital “Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías”.
CONPES	3854	2016	Política Nacional de Seguridad Digital. “Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.”
CONPES	3701	2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa “Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio”
NTC-ISO/IEC	27001	2022	Norma Técnica Colombiana NTC-ISO/IEC 27001 Sistemas de Gestión de la Seguridad de la Información.
NTC-ISO	9001	2015	Norma Técnica Colombiana NTC-ISO 9001 Sistemas de Gestión de la Calidad.
NTC-ISO	22301	2024	Norma Técnica Colombiana NTC-ISO 22301 Sistemas de Gestión de la Continuidad del Negocio.
Modelo	Versión 5	2025	Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas Versión 5 21/04/2025 Ministerio de Tecnologías de la Información y las Comunicaciones
Documento Maestro	Versión 5	2025	Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información Versión 5 21/04/2025 Ministerio de Tecnologías de la Información y las Comunicaciones
Lineamientos	Versión 5	2025	Lineamientos de Roles y Responsabilidades Versión 5 21/04/2025 Ministerio de Tecnologías de la Información y las Comunicaciones

Fuente: Elaboración Propia

5. CONDICIONES GENERALES:

El presente documento se encuentra enmarcado en las directrices establecidas en la Norma NTC-ISO/IEC 27001, en los lineamientos y guías emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y en el Modelo de Seguridad y Privacidad de la Información (MSPI), conforme a lo dispuesto en la Resolución 2277 de 2025, y tiene como propósito fortalecer el mejoramiento continuo del componente de gestión de la seguridad de la información.



Así mismo, el documento se encuentra alineado con el Modelo Integrado de Planeación y Gestión (MIPG), particularmente con la Dimensión de Control Interno y la Dimensión de Gestión con Valores para Resultados, y aporta al Formulario Único de Reporte de Avances de la Gestión (FURAG), en lo relacionado con la implementación, seguimiento y evaluación del MSPI y de la Política de Seguridad Digital.

Lo anterior, con el fin de mitigar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información digital institucional, mediante la implementación, seguimiento y mejora de las estrategias de Seguridad Digital definidas en el presente documento para la vigencia 2026–2027.

6. CONTENIDO

6.1 Estado Actual de la Entidad respecto al Sistema de Seguridad y Privacidad de la Información SGSI

El estado actual del Sistema de Seguridad y Privacidad de la Información de la Entidad evidencia un nivel de cumplimiento parcial frente a los lineamientos establecidos en la Resolución 2277 de 2025 del MSPI, la Norma NTC-ISO/IEC 27001:2022, y los documentos emitidos por el MinTIC, encontrándose el sistema en un nivel de madurez en desarrollo.

La Entidad cuenta con elementos fundamentales de gobernanza, tales como políticas, lineamientos y responsabilidades definidas; no obstante, se identifica la necesidad de fortalecer la claridad e independencia del rol responsable del MSPI, así como la articulación efectiva con las instancias de decisión y control institucional, en concordancia con el MIPG y los criterios evaluados en el FURAG.

En materia de gestión de riesgos de seguridad de la información, se dispone de una metodología documentada; sin embargo, se requiere robustecer el proceso de Selección, Declaración de Aplicabilidad (SOA), garantizando que estos respondan de manera efectiva a los riesgos identificados y que su implementación, seguimiento y evaluación se realicen de forma periódica y sistemática.

Así mismo, los controles de seguridad de carácter organizacional, técnico y humano presentan niveles de implementación desiguales, evidenciándose oportunidades de mejora en su integración, documentación y medición de efectividad.

En cuanto a la gestión de incidentes de seguridad digital, se identifican avances iniciales; no obstante, resulta necesario fortalecer los procedimientos de detección, reporte, atención y cierre de incidentes, así como la articulación con COLCERT, conforme a los lineamientos nacionales de seguridad digital.

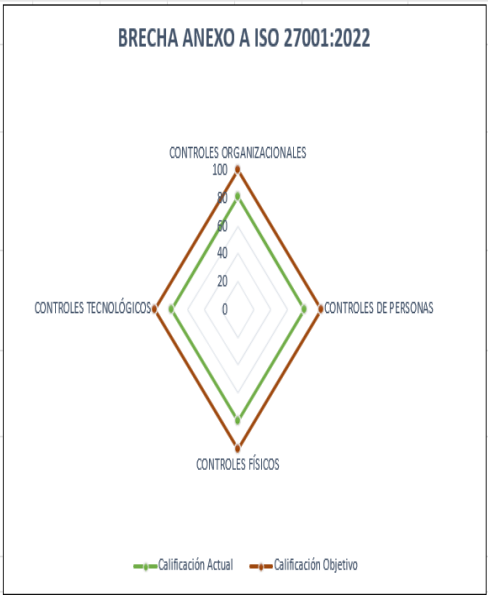
Finalmente, se identifica la necesidad de consolidar los mecanismos de seguimiento, medición y mejora continua, mediante el establecimiento de indicadores, la realización de auditorías internas periódicas y la formulación de planes de mejoramiento que permitan avanzar hacia un mayor nivel de madurez y cumplimiento integral del MSPI.



Grafica 1 Instrumento Madurez MSPI

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2022 ANEXO A

No.	Evaluación de Efectividad de controles			Nivel de Madurez
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	CONTROLES ORGANIZACIONALES	81	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	80	100	GESTIONADO
A.7	CONTROLES FÍSICOS	80	100	GESTIONADO
A.8	CONTROLES TECNOLÓGICOS	80	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		80	100	OPTIMIZADO

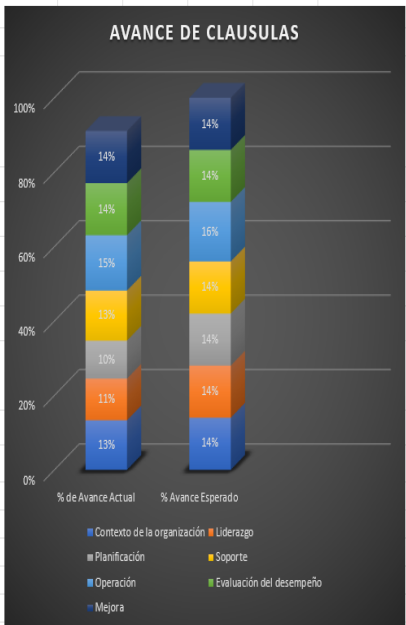


Fuente: Elaboración propia.

Grafica 2 Instrumento Madurez MSPI

AVANCE CLÁUSULAS DEL MODELO DE OPERACIÓN (PHVA)

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	Planificación	Contexto de la organización	13%	14%
		Liderazgo	11%	14%
		Planificación	10%	14%
		Soporte	13%	14%
	Implementación	Operación	15%	16%
	Evaluación de Desempeño	Evaluación del desempeño	14%	14%
	Mejora Continua	Mejora	14%	14%
TOTAL			91%	100%



Fuente: Instrumento MSPI

Respecto a los resultados obtenidos en las políticas de Gobierno Digital y Seguridad Digital en la Medición del Desempeño Institucional, a través del diligenciamiento del Formulario Único de

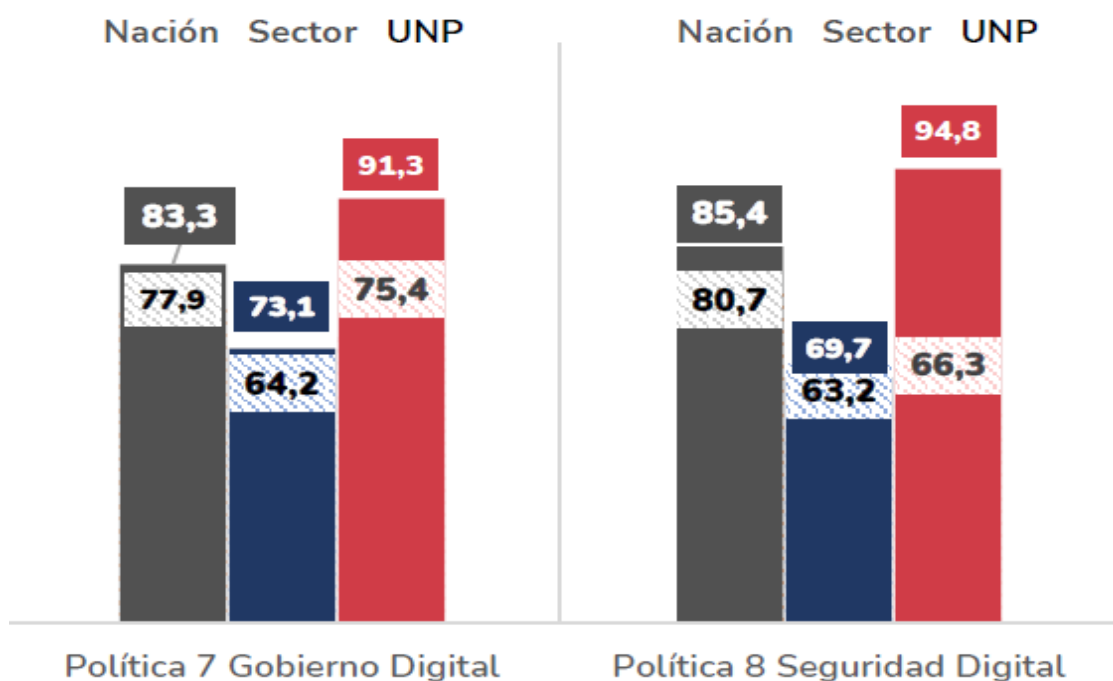


Reporte y Avance de Gestión (FURAG), se evidencia una mejora significativa y sostenida en el desempeño de la Entidad durante la vigencia 2024.

En la política de Gobierno Digital, la Entidad en la vigencia 2024 alcanzó un puntaje de 91,3, superando ampliamente el promedio del sector, que se ubicó en 73,1 puntos. De igual manera, en la política de Seguridad Digital que para la misma vigencia 2024, se obtuvo un resultado de 94,8 puntos, superando de forma considerable el puntaje sectorial de 69,7 puntos.

Estos resultados reflejan el fortalecimiento progresivo de la gestión institucional, derivado de la implementación efectiva de lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), la consolidación del Modelo de Seguridad y Privacidad de la Información (MSPI), la mejora en la gestión de riesgos, la aplicación sistemática de controles de seguridad y el fortalecimiento de los procesos de seguimiento y autoevaluación.

Gráfico 3 Resultados FURAG vigencia 2024



Elaboración propia

Fuente: <https://www1.funcionpublica.gov.co/web/mipg/resultados-medicion>

Por su parte el resultado en la política de Seguridad Digital arrojó un resultado de 94,8 puntos en la vigencia 2024 superando al sector que alcanzó 69,7 puntos.

Para mayor visibilidad en los resultados a continuación se detallan los puntajes de los índices desagregados por estas políticas en la vigencia 2024.



Gráfica 4 Índices Gobierno Digital vigencia 2024:

I11.Gobernanza	I12.Innovación Pública Digital	I13.Arquitectura	I14.Seguridad y Privacidad de la información
100	100	82,0	92,9

I15.Servicios Ciudadanos Digitales	I16.Cultura y apropiación	I17.Servicios y Procesos Inteligentes	I18.Estado abierto
50	100	57,1	97,6

I19.Decisiones basadas en datos	I20.Proyectos de Transformación Digital	I21.Estrategias de Ciudades y Territorios Inteligentes
100	100	NA

Elaboración propia

Fuente: <https://www1.funcionpublica.gov.co/web/mipg/resultados-medicion>

Gráfica 5 Índices Seguridad Digital vigencia 2024

I22.Asignación de Recursos	I23.Implementación Lineamientos de Política	I24.Despliegue de Controles
94,4	93,3	100

Elaboración propia

Fuente: <https://www1.funcionpublica.gov.co/web/mipg/resultados-medicion>

6.2 Descripción del Modelo de Seguridad y Privacidad Información MSPI

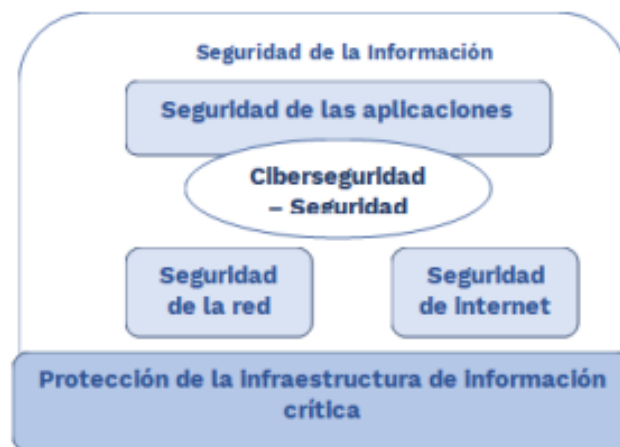
La fase de diagnóstico permite a las entidades establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe realizar un “Diagnóstico” utilizando el “instrumento de evaluación MSPI” con el que se identifica de forma específica los controles implementados, se mide el nivel de madurez de la implementación del modelo de seguridad y privacidad de la información y se obtienen insumos fundamentales para la fase de planificación. Este autodiagnóstico se debe realizar antes de iniciar la fase de planificación y actualizar la información tras terminar la fase de evaluación de desempeño, para identificar los cambios en el nivel de madurez de la implementación del Modelo en la Entidad, el resultado que se obtenga después de la fase de evaluación de desempeño se incluirá como un insumo, en la fase de mejoramiento continuo.



Grafica 6: Ciclo del Modelo de Seguridad y Privacidad de la Información

Fuente https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401770_recurso_1.pdf

La seguridad de la información debe entenderse como un enfoque integral y transversal, sustentado en la articulación de diversos componentes que, de manera coordinada, permiten proteger no solo los sistemas tecnológicos, sino también el factor humano, la infraestructura física, los procesos de desarrollo de software, la gestión del talento humano, la calidad institucional, la relación con proveedores y demás elementos críticos de la organización. En este contexto, se hace necesaria la implementación de estrategias y controles orientados a garantizar la confidencialidad, integridad y disponibilidad de la información, abarcando de forma equilibrada los ámbitos técnico, organizacional y administrativo, y asegurando su aplicación en todos los niveles de la Entidad.

Grafica 7: Relación entre la Ciberseguridad y otros Ámbitos de la Seguridad (Fuente: ISO/IEC 27032)

Fuente https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401770_recurso_1.pdf



6.3 Para Lograr el Cumplimiento del Plan se Definen las Siguientes Etapas:

6.3.1 Contexto

Los elementos externos e internos que son relevantes con las actividades que realiza la Entidad en el desarrollo de su misión y que podrían influir en las capacidades para lograr los objetivos del modelo, alineado con los objetivos estratégicos de la Entidad, teniendo en cuenta procesos necesarios y sus interacciones.

6.3.2 Alcance

El alcance y la aplicabilidad del MSPI en el marco del modelo de operación por procesos de la Entidad. Esta definición debe especificar a qué procesos, recursos humanos, financieros, técnicos y tecnológicos se aplicará la implementación del modelo. Se recomienda iniciar con los procesos misionales, dado su impacto estratégico y su nivel de exposición a riesgos de seguridad y privacidad de la información.

6.3.3 Política del MSPI

Mediante Resolución 2221 de 2025, la UNP actualizó los lineamientos del Modelo de Seguridad y Privacidad de la Información, de acuerdo con lo establecido en el Anexo 1 de la Resolución 2277 de 2025 del Ministerio de Tecnologías de la Información y Comunicaciones - MinTic que establece la base respecto al comportamiento personal y profesional de los servidores públicos, contratistas y demás colaboradores sobre la información obtenida, generada o procesada por la Entidad.

6.3.4 Identificación de Activos de Información

Los activos de información constituyen la base para la identificación y análisis de los riesgos, en la medida en que sobre ellos recae el impacto derivado de la materialización de las amenazas de seguridad y privacidad de la información. La identificación, inventario y clasificación de los activos se realiza conforme a lo establecido en el **Anexo Técnico de la Resolución 2277 de 2025**, los lineamientos del **Modelo de Seguridad y Privacidad de la Información — MSPI a nivel nacional**, y las disposiciones internas adoptadas por la UNP para la gestión de activos de información. Para tal fin, se definen las **categorías de clasificación**, los **roles y responsables del registro y administración de los activos**, así como la **herramienta institucional empleada para su levantamiento, actualización y control**, garantizando trazabilidad y articulación con el SGSI y el inventario de infraestructura crítica cibernética. Conforme a lo establecido en los lineamientos para el inventario y clasificación de activos de información e infraestructura crítica cibernética nacional.



6.4 Estrategia de Seguridad Digital

La Unidad Nacional de Protección UNP establece la estrategia de seguridad digital a Estrategia de Seguridad Digital de la Entidad se encuentra formulada, aprobada e implementada desde la vigencia anterior, en cumplimiento de lo establecido en el artículo 5 de la Resolución 500 de 2021, y se articula de manera complementaria con el Plan de Seguridad y Privacidad de la Información y el SGSI. Su desarrollo se sustenta en los siguientes aspectos:

- **Aprobación mediante acto administrativo**

La Estrategia de Seguridad Digital fue formalizada a través de acto administrativo de carácter general, materializado en la actualización normativa institucional que migró de la Resolución 1774 a la Resolución 2221 de 2025, incorporando los lineamientos vigentes de política de Gobierno Digital y seguridad digital definidos por el Ministerio TIC.

- **Análisis y tratamiento de riesgos de seguridad digital**

La Entidad cuenta con un esquema de gestión de riesgos de seguridad digital que incluye la identificación, análisis, valoración y tratamiento de riesgos, soportado en la matriz de riesgos, el plan de tratamiento y los controles asociados, los cuales se encuentran aprobados y en aplicación desde la vigencia anterior, evidenciando una gestión continua del riesgo.

- **Definición de roles y responsabilidades**

Se dispone de Resolución 0928 de 2025 y matriz de roles y responsabilidades en materia de seguridad digital y seguridad de la información, documentos que fueron actualizados, socializados y puestos en conocimiento de los responsables, bajo el seguimiento de la instancia competente, garantizando claridad en la gobernanza y ejecución de la estrategia.

- **Promoción de la cultura de seguridad digital**

La Estrategia contempla la implementación de principios, lineamientos y acciones orientadas a fortalecer la cultura de seguridad digital y de la información, a través de actividades de difusión, capacitación y concientización dirigidas a servidores públicos y contratistas. Estas actividades se ejecutan de manera periódica y se encuentran incorporadas en el Plan Institucional de Capacitación, destacándose la realización anualmente la Semana de la Ciberseguridad.

- **Alcance sobre las tecnologías de la información y las comunicaciones**

La Estrategia de Seguridad Digital abarca la totalidad de las tecnologías de la información y las comunicaciones utilizadas por la Entidad, incluyendo la adopción y evaluación de nuevas tecnologías y tecnologías emergentes, en concordancia con los lineamientos del Ministerio TIC y las necesidades institucionales, asegurando su articulación con el SGSI.

En consecuencia, la Estrategia de Seguridad Digital se integra como un componente transversal del Plan de Seguridad y Privacidad de la Información, garantizando coherencia



normativa, continuidad en su implementación y fortalecimiento progresivo de la seguridad digital institucional.

Por tal motivo, la Unidad Nacional de Protección UNP orientará sus acciones con las 5 estrategias de seguridad digital como son: liderazgo de la seguridad de la información, la gestión integral de riesgos y su respectivo plan de tratamiento, el seguimiento de controles de seguridad, la gestión y atención de incidentes de seguridad digital, y el desarrollo de estrategias de sensibilización y concientización dirigidas a servidores públicos y contratistas, con el fin de consolidar una cultura de seguridad, mejorar la capacidad de respuesta y asegurar la protección de la información y la continuidad de los servicios institucionales.:

Grafica 8 Estrategia de Seguridad Digital



Fuente: Tomado de MINTIC

- **Liderazgo de seguridad y privacidad de la información**

Mantener el Modelo de Seguridad y Privacidad de la Información (MSPI) en la Entidad, a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.

- **Gestión de Riesgos**

La determinación de los riesgos de seguridad de la información en la UNP se realiza mediante la planificación y valoración definidas, conforme a la Guía para la Administración del Riesgo del DAFP en su versión vigente, con el fin de prevenir o



reducir efectos indeseados. Este proceso se fundamenta en la implementación de controles de seguridad para el tratamiento de los riesgos, los cuales se documentan y gestionan a través del Plan de Tratamiento de Riesgos y demás documentos de soporte del SGSI.

- **Concientización**

Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que se convierta en un hábito, promoviendo y apropiando al interior de la Entidad las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades a todo el personal en seguridad y privacidad de la información.

- **Implementación de controles**

Planificar acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, estas acciones se pueden subdividir en controles tecnológicos y/o administrativos.

- **Gestión de Incidentes**

Gestionar las vulnerabilidades, los incidentes de seguridad de la información y realizar pruebas de continuidad, con el fin de identificar debilidades, evaluar la efectividad de los controles y asegurar la capacidad de respuesta y recuperación de la Entidad, minimizando los impactos ante eventos adversos.

7. META ESTABLECIDA

La meta para la vigencia del Plan de Seguridad y Privacidad de la Información será de 100% de cumplimiento, de acuerdo con la meta definida para cada trimestre.

8. INDICADOR DE MEDICIÓN

Para la gestión del indicador del Plan se realizará un seguimiento a cada una de las Actividades así:

Tabla 1. Indicador del Plan Seguridad y Privacidad de la información

Nombre del indicador	Objetivo	Fórmula	Meta
Cumplimiento del Plan Seguridad y Privacidad de la información	Medir el porcentaje de cumplimiento de las fases definidas en el Plan Seguridad y Privacidad de la información	$\left(\frac{\text{Fases ejecutadas durante el trimestre}}{\text{fases programadas durante el trimestre}} \right) * 100$	100%

Fuente: Elaboración Propia



La meta se desglosa trimestralmente de la siguiente manera:

Tabla 2 Avance Esperado y Meta del Indicador

Trimestre	Avance esperado del trimestre	META ANUAL
I Trimestre	30%	100%
II Trimestre	50%	
III Trimestre	10%	
IV Trimestre	10%	

Fuente: Elaboración Propia

Para promover el cumplimiento de los objetivos se establecen los siguientes indicadores por objetivo destacando que el indicador de medición del Plan Seguridad y Privacidad de la información es el establecido Tabla 1. Plan Seguridad y Privacidad de la información

Tabla 3. Indicadores Internos por Objetivos

Nombre del Indicador	Objetivo	Formula	Meta Trimestral
Porcentaje diagnóstico del sistema	Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la Entidad.	(Cantidad de componentes implementados/ cantidad de componentes evaluados) *100%	100%
Porcentaje de controles evaluados	Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.	(Número de controles evaluados / Numero de controles definidos) *100%	100%
Porcentaje de sensibilizaciones realizadas	Lograr una alta cobertura de sensibilización del SGSI en servidores públicos y contratistas.	(cantidad de sensibilizaciones realizadas/Cantidad total de sensibilizaciones planificadas en la fase) *100%	100%
Porcentaje de documentos actualizados y creados	Actualizar oportunamente los documentos del MSPI de acuerdo con las necesidades institucionales y los cambios normativos y operativos	(Cantidad de documentos creados o actualizados/Cantidad de documentos definidos) *100%	100%

Fuente: Elaboración Propia



9. HOJA DE RUTA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y ESTRATEGIA DIGITAL (CRONOGRAMA)

PLAN DE SEGURIDAD DE LA INFORMACIÓN				PROGRAMACIÓN 2026											
Objetivo	Fases	Recursos	Entregable	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la Entidad.	Aprobación del Plan de Seguridad de la Información por el Comité Institucional de Gestión y Desempeño	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información. *Constancia secretarial	*constancia secretarial	30%											
	Realizar la evaluación con la herramienta de autodiagnóstico de MinTic	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Archivo de autodiagnóstico *Acta de reunión	*Acta de reunión *Archivo autodiagnóstico												
	Realizar un análisis de vulnerabilidades de infraestructura	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Informe de Análisis de vulnerabilidades de Infraestructura	*Informe de Análisis de vulnerabilidades de Infraestructura												
	Realizar un análisis de vulnerabilidades de Sistemas de Información	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Informe de Análisis de vulnerabilidades de Sistemas de Información	*Informe de Análisis de vulnerabilidades de Sistemas de Información												
	Realizar un análisis de inteligencia de amenazas	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Informe de Inteligencia de Amenazas	*Informe de Inteligencia de Amenazas												



PLAN DE SEGURIDAD DE LA INFORMACIÓN				PROGRAMACIÓN 2026											
Objetivo	Fases	Recursos	Entregable	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información	Actualizar la declaración de aplicabilidad dando cumplimiento a los requisitos	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Documento Declaración de Aplicabilidad (SOA)	*Documento Declaración de Aplicabilidad SOA – GIN-FT-61				50%								
	Programar muestra de controles críticos y estándar de controles	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Informe programación y planificación de muestra de controles críticos y estándar de controles	*Informe programación y planificación de muestra de controles críticos y estándar de controles												
	Realizar un análisis de vulnerabilidades de infraestructura	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Informe	*Informe de Análisis de vulnerabilidades de Infraestructura												
	Realizar un análisis de vulnerabilidades de Sistemas de Información	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Informe de Análisis de vulnerabilidades de Sistemas de Información	*Informe de Análisis de vulnerabilidades de Sistemas de Información												
	Realizar un análisis de inteligencia de amenazas	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Informe de Inteligencia de Amenazas	*Informe de Inteligencia de Amenazas												



PLAN DE SEGURIDAD DE LA INFORMACIÓN				PROGRAMACIÓN 2026											
Objetivo	Fases	Recursos	Entregable	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
Lograr una alta cobertura (Servidores públicos y/o Contratistas) de sensibilización del SGSI en servidores públicos y contratistas.	Realizar (3) sesiones presenciales y/o virtuales dirigidas a servidores públicos y contratistas, en las que se socialicen los principios del SGSI, las políticas de seguridad de la información, roles y responsabilidades, y buenas prácticas para el manejo seguro de la información.	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Cronograma de las jornadas (fechas, modalidad, población objetivo). *Convocatorias enviadas (correos electrónicos, invitaciones institucionales). *Material de socialización: Presentaciones (PPT) y/o Listados de asistencia (Firmas (presencial) Reportes de asistencia de la plataforma (virtual) y/o Actas o memorias de la jornada, donde se registre: *Evaluaciones de conocimiento o encuestas de satisfacción (si se realizan).	*Cronograma de las jornadas *Convocatorias enviadas *Material de socialización *Evaluaciones de conocimiento o encuestas de satisfacción							10%					
	Implementar una campaña de comunicación interna mediante correos electrónicos, intranet, piezas gráficas y mensajes informativos, orientada a reforzar la cultura de seguridad de la información y a sensibilizar de manera continua sobre riesgos, controles y obligaciones del SGSI.	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Correos institucionales periódicos *Publicaciones en los diferentes canales de comunicación *Piezas gráficas (infografías) *Mensajes cortos o boletines informativos	*Correos institucionales periódicos *Publicaciones en los diferentes canales de comunicación *Piezas gráficas *Mensajes o boletines informativos												



PLAN DE SEGURIDAD DE LA INFORMACIÓN				PROGRAMACIÓN 2026											
Objetivo	Fases	Recursos	Entregable	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
	Realizar un análisis de vulnerabilidades de infraestructura	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Informe de Análisis de vulnerabilidades de Infraestructura	*Informe de Análisis de vulnerabilidades de Infraestructura												
	Realizar un análisis de vulnerabilidades de Sistemas de Información	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Informe Análisis de vulnerabilidades de Sistemas de Información	*Informe Análisis de vulnerabilidades de Sistemas de Información												
	Realizar auditoría Interna de la norma ISO/IEC27001	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Plan de auditoría *Lista de chequeo *Informe auditoría en el software de DEMING	*Plan de auditoría *Lista de chequeo *Informe auditoría												
	Realización de una inteligencia de amenazas	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Informe de Inteligencia de Amenazas	*Informe de Inteligencia de Amenazas												
Actualizar y crear los documentos para la madurez del Sistema	Revisar y actualizar el Análisis de Impacto al Negocio (BIA) con el fin de identificar procesos críticos, tiempos máximos de recuperación (RTO), puntos objetivos de recuperación (RPO) e impactos operativos,	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Documento BIA actualizado y aprobado y formalizado en la intranet de la Entidad.	*Documento BIA actualizado y aprobado y formalizado en la intranet de la Entidad. *Constancia secretarial										10%		



PLAN DE SEGURIDAD DE LA INFORMACIÓN				PROGRAMACIÓN 2026											
Objetivo	Fases	Recursos	Entregable	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
	legales y reputacionales, considerando cambios organizacionales, tecnológicos y normativos.	*Matriz de procesos críticos/Acta de revisión y validación													
	Revisar y actualizar la política general y demás lineamientos buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad.	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información. Documento Acto administrativo 2221/2025 actualizado.	Documento Acto administrativo actualizado.												
	Actualizar el Protocolo de Contingencia para Atención de Crisis en tecnología y Seguridad de la Información con base en los resultados del BIA, incorporando escenarios de interrupción, estrategias de continuidad, roles y responsabilidades, procedimientos de respuesta y recuperación.	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Plan de Continuidad actualizado *Acta de aprobación *Relación de responsables y contactos de emergencia	*Plan de Continuidad de negocio actualizado *Acta de aprobación *Relación de responsables y contactos de emergencia												



PLAN DE SEGURIDAD DE LA INFORMACIÓN				PROGRAMACIÓN 2026											
Objetivo	Fases	Recursos	Entregable	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
	Revisar y actualizar documentos del sistema que apoye a la operación para asegurar su alineación con el contexto de la Entidad, los requisitos legales y normativos aplicables y la estrategia institucional.	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Documentos actualizados (3) *Actas de aprobación *Registros de divulgación interna	*Documentos actualizados (3) *Actas de aprobación *Registros de divulgación interna												
	Realizar pruebas de continuidad para infraestructura	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Informe realización de pruebas de continuidad para infraestructura.	*informe realización de pruebas de continuidad para infraestructura.												
	Realizar pruebas de continuidad para sistemas de información	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *informe realización de pruebas de continuidad para sistemas de información.	informe realización de pruebas de continuidad para Sistemas de información.												
	Realizar Contratar auditoría Externa de la norma SO/IEC27001	Servidor público y/o contratista designado al sistema de gestión de seguridad de la información *Plan de auditoría *Informe de auditoría	*Plan de auditoría *informe de auditoría												



10. DOCUMENTOS RELACIONADOS:

- GTE-MD-01 Modelo de Seguridad y Privacidad de la Información.
- GIN-FT-61 Declaración de Aplicabilidad SOA.

11. CONTROL DE CAMBIOS

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
00	Creación del Plan Seguridad y Privacidad de la Información	31/01/2019	01
01	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2020	31/01/2020	02
02	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2021	20/01/2021	03
03	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2022	20/01/2022	04
04	Actualización de las fechas propuestas en el cronograma de actividades del plan de Seguridad y Privacidad de la Información y desglose de la meta propuesta en el indicador, por valores acumulativos de porcentaje en cada uno de los semestres.	17/05/2022	05
05	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia, se hace claridad con relación a la metodología de trabajo y actualización de las actividades en el cronograma para el Anexo y el plan de Seguridad y Privacidad de la Información para la vigencia 2024.	29/01/2024	06
06	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia, enmarcado en las directrices contenidas en la Norma NTC-ISO/IEC ISO 27001:2022 y las Guías publicadas por MinTIC	20/03/2024	07



VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
07	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2025, se incluyen las actividades de Estado Actual del Sistema de Gestión en Seguridad y Privacidad de la Información, Proceso de Seguridad y Privacidad de la Información, Política general de Seguridad y Privacidad de la Información, Ámbito general de Seguridad y Privacidad de la Información. Se incluye el cronograma en el contenido del plan.	31/01/2025	08
08	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2026	26/01/2026	09

12. CRÉDITOS:

FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN DEL DOCUMENTO	
Elaboró: Nombre: Julian Camilo Bejarano Rojas Cargo: Contratista Oficina de Tecnologías y Sistemas de Información	APROBADO PLATAFORMA TECNOLÓGICA
Elaboró: Nombre: Luz Anyela Avila Gomez Cargo: Contratista Oficina de Tecnologías y Sistemas de Información	
Elaboró: Nombre: John Anderson Hernandez Correa Cargo: Contratista Oficina de Tecnologías y Sistemas de Información	
Elaboró: Nombre: Elsa Marlen Baracaldo Huertas Cargo: Contratista Grupo de Gestión Integrada y Mejora– Oficina Asesora de Planeación	
Revisó: Nombre: Javier Francisco Rodríguez Moreno Cargo: Jefe Oficina de Tecnologías y Sistemas de Información (E)	
Aprobó: Nombre: Sandra Milena Ardila Cubides Cargo: Director (a) General (E)	
FIRMA DE OFICIALIZACIÓN DEL DOCUMENTO- SISTEMA INTEGRADO DE GESTIÓN MIPG-SIG	
Oficializó: Nombre: Javier Francisco Rodríguez Moreno Cargo: Jefe Oficina Asesora de Planeación	APROBADO PLATAFORMA TECNOLÓGICA

